kaveh rajabi

Web Penetration Tester - Security Analyst

درباره من

من کاوه رجبی هستم؛ Web Penetration Tester و Security Analyst.
مسیر کاریم رو از Help Desk شروع کردم و بعد وارد SOC شدم؛ جایی که توی شیفت‌ها، یاد گرفتم چطور با دقت بالا Incident هارو از اول تا آخر مستند و پیگیری کنم.

تا حالا گواهینامه‌های CEH، LPIC1، Network+ و SEC542 رو گرفتم . دوره‌های CEH و SEC542 رو در آموزشگاه نورانت با تدریس استاد علیرضا راستی‌دوست گذروندم.
در بخش SOC Tier 1 تجربه کار شیفتی، تحلیل هشدارهای امنیتی، بررسی ترافیک مشکوک، کار با SIEM و مدیریت تیکت‌های امنیتی داشتم. همیشه تلاش می‌کردم تیکت‌هارو با دقت، تحلیل واقعی و توضیحات کامل ثبت کنم تا خروجی کارم برای تیم بالادستی ارزشمند و قابل استفاده باشه. همین تجربه باعث شد دید عملی‌تری نسبت به تهدیدها، رفتار سیستم‌ها و Incidentها پیدا کنم.

ترکیب تجربه‌ی SOC و علاقه‌ی اصلی‌م به پنتست باعث شده بتونم هم از نگاه دفاعی سیستم رو بفهمم و هم از نگاه تهاجمی تحلیل کنم. دنبال محیطی هستم که بتونم در کنار تیم، رشد کنم و تجربه عملی بیشتری کسب کنم. در عین حال Bug Bounty برام یک مسیر یادگیری روزمره و شخصیه که باعث می‌شه همیشه به‌روز بمونم.

تجربه‌های کاری

HELP DESK

رایان سیستم | خرداد ۱۳۹۷ تا فروردین ۱۳۹۹

(SOC (TIER1

امن پردازان کویر (APK) | مرداد ۱۴۰۳ تا تیر ۱۴۰۴

. مانیتورینگ و تحلیل رخدادهای امنیتی

. پاسخ به Incidentها و بررسی لاگ‌ها

. شناسایی تهدیدات و کاهش False Positive

. گزارش‌نویسی و مستندسازی امنیتی

Bug Bounty Hunter

Independent | خرداد ۱۴۰۲ تا حالا

شناسایی و گزارش چند آسیب‌پذیری تأییدشده در پلتفرمBugCrowd .

کشف آسیب‌پذیری Account Squatting در linktr.ee و نقص مشابه در Pinterest.

گزارش Server Security Misconfiguration تأییدشده با اولویت P5 در یک برنامه رسمی.

تخصص در Recon، شناسایی misconfigurationها، و تحلیل امنیتی در حوزه XSS, OAuth Abuses, API Security.

اطلاعات تماس

تماس از طریق جابینجا

اطلاعات شخصی

سال تولد: ۱۳۷۵
وضعیت سربازی: پایان خدمت
وضعیت تأهل: متأهل

زبان‌ها

انگلیسی (حرفه‌ای)
فارسی (زبان مادری)

اطلاعات تماس

تماس از طریق جابینجا

اطلاعات شخصی

سال تولد: ۱۳۷۵
وضعیت سربازی: پایان خدمت
وضعیت تأهل: متأهل

زبان‌ها

انگلیسی (حرفه‌ای)
فارسی (زبان مادری)

مهارت در تهیه گزارش‌های امنیتی استاندارد شامل PoC، مراحل بازتولید و تحلیل Impact.

آشنایی با ابزارهای امنیتی: Burp Suite, Metasploit, Nuclei, FFUF, Amass, Subfinder.

سوابق تحصیلی

ریاضی و فیزیک (دیپلم)
پیش دانشگاهی علوم | ۱۳۸۲ تا ۱۳۹۳

رشته دانشگاهیم مهندسی صنایع بود که قبل از خدمت انصراف دادم.

فناوری اطلاعات - اینترنت و شبکه های گسترده (کاردانی)
دانشکده داده پردازی ایران | ۱۴۰۲ تا ۱۴۰۴

مهندسی فناوری اطلاعات-فناوری اطلاعات (کارشناسی)
مرکز آموزش علمی کاربردی انفورماتیک ایران | ۱۴۰۴ (در حال تحصیل)

مهارت‌های حرفه‌ای

. OWASP . Webapp Pentesting . CEH . LPIC1 . NETWORK+
OWASP WSTG . Active Directoy . SEC542 . sec511 . Bug Hunting